HO Van Khanh

19,5

# DM: Introduction à la Vérification

## Exo 1 :

$$\phi = AF(b \wedge \neg a) \Rightarrow AF\,A(b\ W(\neg a \wedge \neg b))$$

### 1) Mettre en forme ENF :

$$\phi = AF(b \wedge \neg a) \Rightarrow AF\,A(b\ W(\neg a \wedge \neg b))$$

$$\Leftrightarrow \phi \equiv \underbrace{\neg AF(b \wedge \neg a)}_{\phi_1} \vee \underbrace{AF\,A(b\ W(\neg a \wedge \neg b))}_{\phi_2}$$

$$\phi_1 \equiv EG(\neg b \vee a)$$

$$\phi_2 \equiv \neg EG(\neg A(b\ W(\neg a \wedge \neg b)))$$

$$\equiv \neg EG(E((\underbrace{b \wedge (a \vee b)}_{\equiv b})\ U\ (\underbrace{\neg b \wedge (a \vee b)}_{\equiv a \wedge \neg b})))$$

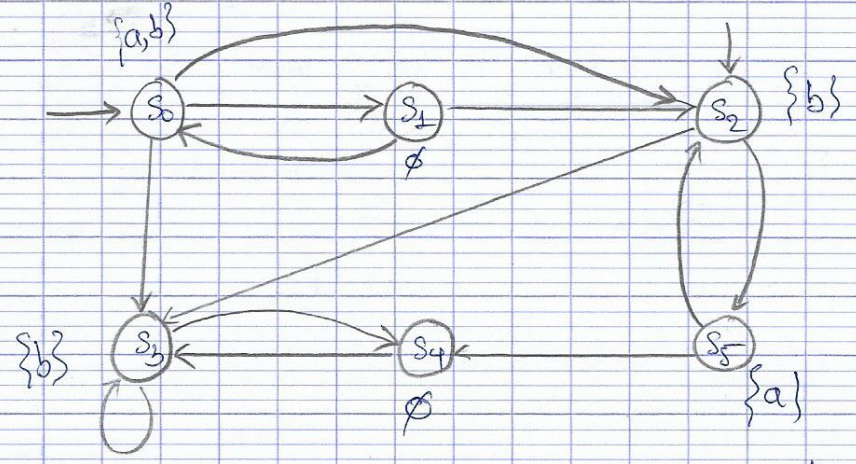
(Après le cours, on a vu que :

$$\neg A(\phi\ W\ \psi) = E((\phi \wedge \neg\psi)\ U\ (\neg\phi \wedge \neg\psi))\ )$$

$$\Rightarrow \phi = EG(\neg b \vee a) \vee \neg EG(E(b \wedge (a \vee b))\ U\ (\neg b \wedge (a \vee b))))$$

$$= EG(\neg b \vee a) \vee \neg EG(E(b\ U\ (\neg b \wedge a)))$$ ✓

### 2) Calculer Sat(¥φ)




$$\phi = \underbrace{EG(\neg b \vee a)}_{\phi_1} \vee \neg \underbrace{EG(\overbrace{E(b \cup (\neg b \wedge a))}^{\phi_2})}_{\phi_3 \text{ (la négation n'est pas inclus)}}$$

$$\Rightarrow Sat\,\phi = Sat(\phi_1 \vee \neg \phi_3)$$
$$= Sat(\phi_1) \cup S \setminus Sat(\phi_3)$$

+) Calculons $Sat(\phi_1)$ : $\phi_1 = EG(\neg b \vee a)$.

Compteur de # successeur

$T = \{\overset{3}{s_0}, \overset{2}{s_5}, \overset{2}{s_1}, \overset{1}{s_4}\}$

$V = \{s_2, s_3\}$

1ère itération : on regarde $s_2$, $pred(s_2) = \{s_0, s_1, s_5\}$

$\Rightarrow T = \{s_0, s_1, s_5, s_4\}$
$\quad\quad 2\ 1\ 1\ 1$

$V = \{s_3\}$.

2è itération : $s_3$ ; $pred(s_3) = \{s_0, s_2, s_4, s_3\}$ (à T)

$\Rightarrow T = \{s_0, s_1, \cancel{s_5}, s_4\}$
$\quad\quad 1\ 1\ 1\ 0$

$V = \{s_4\}$

3ème itération : $s_4$, pred $(s_4) = \{s_3, s_5\}$ ($s_3 \notin T$)

$T = \{s_0, s_1, \cancel{s_5}\}$

$1 \quad 1 \quad 0$

$V = \{s_5\}$

4ème itération : $s_5$, pred $(s_5) = \{s_2\}$ ($s_2 \notin T$)

$\Rightarrow$ return $T = \{s_0, s_1\}$

$\Rightarrow$ $\boxed{Sat\ \phi_1 = \{s_0, s_1\}}$

$\rightarrow$ Calculons $Sat\ \phi_2$ avec $\phi_2 = E(b\ U(\neg b \wedge a))$

$V = Sat(\neg b \wedge a) = \{s_5\}$.

$T = \{s_5\}$

1ère itération : on regarde $s_5$, pred $(s_5) = \{s_2\}$.

$s_2 \not\models b \Rightarrow V = \{s_2\}$

$T = \{s_5, s_2\}$.

2ème itération : $s_2$, pred $(s_2) = \{s_0, s_1, s_5\}$.

$s_1 \not\models b$

$s_0 \not\models b$

$s_5 \in T$

$\Rightarrow V = \{s_0\}$

$T = \{s_5, s_2, s_0\}$.

3ème itération :

$s_0$, pred $(s_0) = \{s_1\}$

$s_1 \not\models b$.

$\Rightarrow V = \phi$

$T = \{s_0, s_2, s_5\}$.

$\Rightarrow$ $\boxed{Sat\ \phi_2 = \{s_0, s_2, s_5\}}$

↦ Calculons $Sat(\phi_3) = Sat(EG\,\phi_2)$

avec $\phi_2 = EG(E(b\,U(\neg b \wedge a)))$

$T = Sat\,\phi_2 = \{s_0^3, s_2^2, s_5^2\}$

$V = \{s_1, s_3, s_4\}$

1ère itération : $s_1$, $pred(s_1) = \{s_0\}$.

$s_0 \in T$

$\Rightarrow T = \{s_0^2, s_2^1, s_5^2\}$

$V = \{s_3, s_4\}$

2è itération : $s_3$, $pred(s_3) = \{s_0, s_3, s_4, s_2\}$

$s_0, s_2 \in T$ , $s_3, s_4 \notin T$ ✓

$\Rightarrow T = \{s_0^1, s_2^1, s_5^2\}$

$V = \{s_4\}$.

3è itération : $s_4$, $pred(s_4) = \{s_3, s_5\}$

$s_5 \in T$

$\Rightarrow T = \{s_0^1, s_2^1, s_5^1\}$

$V = \{\phi\}$

$\Rightarrow$ $\boxed{Sat\,\phi_3 = \{s_0, s_2, s_5\}}$.

↦ Donc, on a dit que

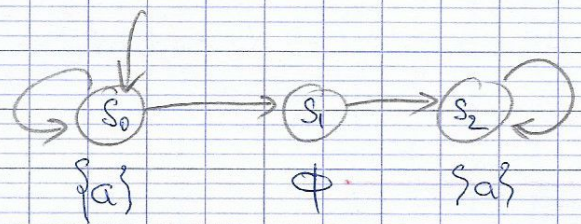
$Sat\,\phi = Sat\,\phi_1 \cup S \setminus Sat(\phi_3)$

$\Rightarrow Sat\,\phi = \{s_0, s_1\} \cup \{s_1, s_3, s_4\}$.

$\Rightarrow Sat\,\phi = \{s_0, s_1, s_3, s_4\}$. ✓

## Exo 2 :

1) $AF\,AXa$ n'est pas équivalent à $FXa$.
Prenons ce TS :




à partir de $s_0$
$S \models FXa$ car toute exécution $\models FXa$
$S \not\models AFAXa$ car l'exécution $s_0 \to s_0 \to \dots$ a l'état $s_0 \not\models AXa$.

✓

2) $AF(a \wedge AFb)$ et $F(a \wedge Fb)$
On va mq : $S \models AF(a \wedge AFb) \Leftrightarrow S \models F(a \wedge Fb)$
($\Rightarrow$) Supposons que le TS $S \models AF(a \wedge AFb)$
$\Rightarrow$ Pour toute exécution à partir de $s_0$, il existe $i$, $s_i \to s_{i+1} \dots \models (a \wedge AFb)$.
$\Rightarrow s_i \models a \wedge s_i \models AFb$.
$\Rightarrow$ Pour toute exécution à partir de $s_i$,
$\exists n : \pi : s_i \xrightarrow{*} s_n : s_n \models b$.
$\Rightarrow$ Pour toute exécution à partir de $s_0$, on peut trouver (i, une telle couple $(i, n)$ tq : $s_0 \xrightarrow{*} s_i \xrightarrow{*} s_n$
$\models a \wedge Fb$ $\models b$
$\Rightarrow S \models F(a \wedge Fb)$

✓

($\Leftarrow$) Supposons que $S \models F(a \wedge Fb)$
Il nous faut montrer que pour toute exécution à partir de $s_0$, $\exists i, n$ tq $s_0 \xrightarrow{*} s_i \xrightarrow{*} s_n$
$\models a \wedge Fb$ $\models b$

or comme $S \models F(a \wedge Fb)$

Toute exécution de $S \not\models F(a \wedge Fb)$

$\Rightarrow$ $\forall$ toute exec $\exists i : s_0 \xrightarrow{*} s_i \ldots$

$\models a \wedge Fb$.

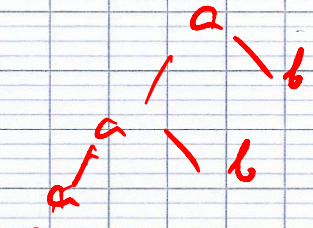
$\Rightarrow \exists i, n, \; s_0 \xrightarrow{*} \underbrace{s_i} \xrightarrow{*} \underbrace{s_n} \ldots$ ($\forall$ toute exécution)

$\models a \wedge Fb$ $\quad \models b$.

(V)

$\Rightarrow S \not\models AF(a \wedge AFb)$

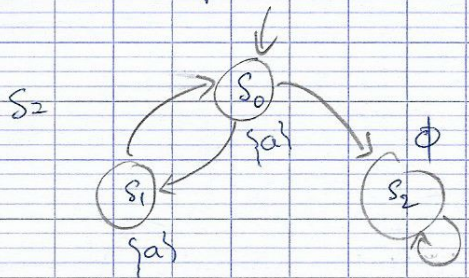
Il faut montrer que




n'est pas possible

3) $EGAXa$ et $GXa$

Prenons cet exemple :




$S \models EGAXa$ grâce à $s_0 \to s_1 \to s_0 \to s_1 \ldots$

$S \not\models GXa$ car $s_0 \to s_2 \to s_2 \ldots \not\models GXa$.

✓

## Exo 3 :

1) $Sat(A(\phi \cup \psi))$ est le plus petit ensemble $T \subseteq S$ tq :

i) $Sat(\psi) \subset T$

ii) $\{ s \in Sat(\phi) : post(s) \subseteq T \} \subseteq T$.

Preuve : On va montrer que :

1. $Sat(A(\phi \cup \psi))$ satisfait i) et ii)
2. Tout T qui satisfait i) et ii) inclut $Sat(A(\phi \cup \psi))$

(1) - Soit $x \in Sat(\psi)$

$\Rightarrow s \models \psi$

$\Rightarrow s \models A(\phi \cup \psi)$ (def.)

$\Rightarrow s \in Sat(A(\phi \cup \psi))$

$\Rightarrow Sat(\psi) \subset Sat(A(\phi \cup \psi))$ ✓

- Si $s \in Sat(\phi)$ et $post(s) \subseteq Sat(A(\phi \cup \psi))$

$\forall s' \in post(s), s' \models A(\phi \cup \psi)$

$\Rightarrow s \models A(\phi \cup \psi)$

$\Rightarrow s \in Sat(A(\phi \cup \psi))$

$\Rightarrow Sat(A(\phi \cup \psi))$ satisfait i) et ii) ✓

(2) Il reste à montrer que $Sat(A(\phi \cup \psi))$ est le plus petit ensemble.

Soit T un ensemble qui satisfait i) et ii)

On va montrer que $Sat(A(\phi \cup \psi)) \subseteq T$.

$\Leftrightarrow \forall s \in Sat(A(\phi \cup \psi)), s \in T$.

Comme $s \in Sat(A(\phi \cup \psi))$

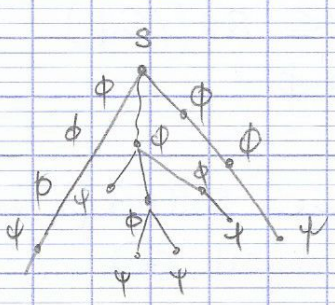
$\Rightarrow s \models A(\phi \cup \psi)$

$\rightarrow$ soit $s \models \psi \Rightarrow s \in T$

soit $\{ \forall s' \in post(s), s' \models A(\phi \cup \psi)$ (*)

$s \models \phi \Rightarrow s \in Sat(\phi)$

En fait, si on déplie le notre SI, on peut obtenir un arbre comme ci-dessous (à partir de l'état s) :




On va monter de bas en haut. ✓

On part depuis tous les états satisfaisant $\psi$ dans toutes les exécutions à partir de $s$, notons $S_n$ l'ensemble de ces états.

$\forall s_n \in S_n$, $s_n \in Sat(\psi)$ donc $s_n \in T$ par (i)

$\Rightarrow S_n \subseteq T$.

Les prédécesseurs des états dans $S_n$, notons $S_{n-1} \subseteq Sat(\phi)$ (par déf. $A(\phi \cup \psi)$)

et $(\forall) s_{n-1} \in S_{n-1}$, $post(s_{n-1}) \subseteq T$

$\Rightarrow S_{n-1} \subseteq T$. (par (ii))

Pour la même raison, en remontant l'arbre on obtient $S_{n-2} \subseteq T$

$\vdots$

$post(s) = S_1 \subseteq T$

$\{s\} = S_0 \subseteq T$

$\Rightarrow s \in T$

$\Rightarrow Sat(A(\phi \cup \psi)) \subseteq T$ □. ✓ +.5.

2. Montrer que :

$Sat(AG\phi)$ est le plus grand ensemble $T \subseteq S$ qui satisfait :

(*) $T \subseteq \{ s \in Sat(\phi) : post(s) \subseteq T \}$.

(i) Montrons que $Sat(AG\phi)$ satisfait (*)

Soit $s \in Sat(AG\phi)$.

$\Rightarrow s \models AG\phi$

par def. AG $\Rightarrow$ $\begin{cases} s \models \phi \\ \forall s' \in post(s),\ s' \models AG\phi \Rightarrow s' \in Sat(AG\phi) \end{cases}$

$\Rightarrow$ $\begin{cases} post(s) \subseteq Sat(AG\phi) \\ s \in sat\ \phi \end{cases}$ ✓

(ii) Montrons que $Sat(AG\phi)$ est le plus grand ensemble $T \subseteq S$ satisfait (*).

Soit $s \in T$, on va montrer que $s \in Sat(AG\phi)$.

$s \in T \Rightarrow s \in Sat\ \phi$ et $post(s) \subseteq T$

$\Rightarrow s \models \phi$ et $\forall s' \in post(s)$, $s' \in T$

Comme $s' \in T \Rightarrow s' \models \phi$ et $\forall s'' \in post(s')$, $s'' \in T$

En ...

En fait, $\forall$ exécution à partir de $s$, on a :

$s \to s' \to s'' \to \dots$

$\phi \quad \phi \quad \phi$

$\Rightarrow$ Tous les sommets accessibles à partir de $s \models \phi$.

$\Rightarrow s \models AG\phi$.

$\Rightarrow s \in Sat(AG\phi)$. ✓

3). Montrer que :

$Sat(A(\phi W \psi))$ est le plus grand ensemble $T \subseteq S$ satisfait :

(*) $T \subseteq Sat(\psi) \cup \{s \in Sat(\phi) : post(s) \subseteq T\}$.

(i) Montrons que $Sat(A(\phi W \psi) \models (*)$.

Premièrement, par définition, $s \in Sat(A(\phi W \psi))$

$\Rightarrow s \models A(\phi W \psi)$

$\Rightarrow$ [soit $s \models \psi \Rightarrow s \in Sat(\psi)$

soit $s \models \phi$ et $\forall s' \in post(s)$, $s' \models A(\phi W \psi)$

$\Downarrow$

$s \models \phi$ et $post(s) \subseteq Sat\ A(\phi W \psi)$

$\Rightarrow$ $s \in Sat(\Psi) \cup \{ s \in Sat(\phi) : post(s) \subseteq Sat A(\phi W \Psi) \}$

$\Rightarrow$ $Sat(A(\phi W \Psi))$ satisfait $(*)$. ✓

(ii) Montrons que $Sat(A(\phi W \Psi))$ est le plus grand ensemble $T$.

Soit $T$ satisfait $(*)$ et $s \in T$.

On va montrer que $s \in Sat(A(\phi W \Psi))$

$s \in T \Rightarrow s \in Sat(\Psi) \cup \{ s \in Sat(\phi) : post(s) \subseteq T \}$.

$\Rightarrow s \in Sat \Psi$ ou $: s \models \phi$ et $\forall s' \in post(s), s' \in T$.

$\Downarrow$

$\in Sat A(\phi W \Psi)$ $\qquad$ $(**)$

$(**) \Leftrightarrow s' \models \Psi$ ou $\forall s'' \in post(s'), s'' \in T$.

En effet, pour tout exécution issue de $s$, on a :

$s \to s \to s_2 \to \dots s_n \to \dots$

$\phi \quad \phi \quad \phi$

(iii) sur cette exécution, soit il existe un état $s_n \models \Psi$,

soit non et $s_n \models \phi$ et tous les états accessibles à partir de $s_n \models \phi$

$\Rightarrow s \models \& A(\phi W \Psi)$ car (iii) est valide $\forall$ exécution.

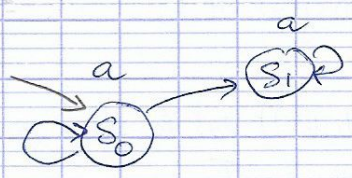
$\Rightarrow s \in Sat(A(\phi W \Psi))$. ✓

Exo 4 :

1) Soit $\phi$ une formule ECTL.
Soit $S_1, S_2$ deux systèmes de transitions et $S_1 \subseteq S_2$.
Supposons que $S_1 \models \phi$.
$\Rightarrow$ Tous les états initiaux $s$ de $S_1$ doit $\models \phi$.
En observant, on peut voir que toutes les formules de ECTL n'utilisent que EX, EU, EG (les "connecteurs" existentiels temporaire) avec la négation appliquée au niveau des propositions atomiques.
Donc à partir d'un état, il nous suffit de trouver une exécution (et pas toute comme pour les connecteurs universels temporaires AG, AU, AX) qui satisfait la formule $\phi$, donc cette état satisfait bien $\phi$.
Autrement dit, $\forall s \in S_1$ :
S'il existe une exécution :
$\pi : S \to s_1 \to s_2 \to \dots$ satisfait $\phi$
$\Rightarrow S \models \phi$ (avec $\phi$ de ECTL).
or, comme $S_1 \subseteq S_2$
$\Rightarrow$ Tous les exécutions issues des états initiaux de $S_1$ qui satisfont $\phi$ existent aussi dans $S_2$ ($\to_1 \subseteq \to_2$, $I_1 = I_2$, $L_1(s) = L_2(s)$ $\forall s \in S_1$)
$\Rightarrow$ les états initiaux de $S_2 \models \phi$.
$\Rightarrow S_2 \models \phi$. ✓

2) Prenons la formule CTL AG a.
Supposons qu'il existe une formule $\phi$ de ECTL équivalente à AG a.

Prenons le ST $S$ qui est définie comme ci-dessous :

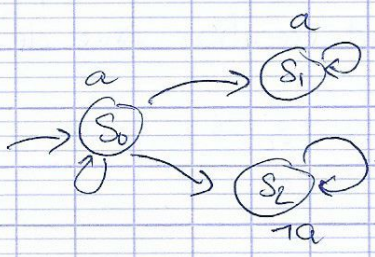



$S$

C'est clair que $S \not\models AGa$.

$\Rightarrow S \models \phi$ car $AGa$ et $\phi$ sont équivalentes par l'hypothèse.

Prenons maintenant le ST $S'$ tel que $S \subseteq S'$ :




Par la question 1, on peut en déduire que

$S' \models \phi$ car $S \subseteq S'$. (ECTL)

$\Rightarrow S' \not\models AGa$ (CTL)

or l'exécution $S_0 \to S_2 \to S_2 \ldots \not\models AGa$.

$\Rightarrow$ Contradiction.

$\Rightarrow$ Il n'existe pas une formule ECTL équivalente à $AGa$.

$\Rightarrow$ Il existe des formules CTL qui ne sont équivalentes à aucune formule ECTL.

✓

super